Docket No.: 08223/000S102-US0
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Letters Patent of:
Brad Kollmyer et al.

Patent No.: 7,165,175

Issued: January 16, 2007

For: APPARATUS, SYSTEM AND METHOD FOR SELECTIVELY ENCRYPTING DIFFERENT PORTIONS OF DATA SENT OVER A NETWORK

REQUEST FOR CERTIFICATE OF CORRECTION
PURSUANT TO 37 CFR 1.323 AND 1.322

Attention: Certificate of Correction Branch
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Upon reviewing the above-identified patent, Patentee noted typographical errors which should be corrected. A listing of the errors to be corrected is attached.

The typographical errors marked with an "A" on the attached list are found in the application as filed by applicant. Please charge our Credit Card in the amount of $100.00 covering the fee set forth in 37 CFR 1.20(a).

The typographical errors marked with a "P" on the attached list are not in the application as filed by applicant. Also given on the attached list are the documents from the file history of the subject patent where the correct data can be found.

The errors now sought to be corrected are inadvertent typographical errors the correction of which does not involve new matter or require reexamination.

Transmitted herewith is a proposed Certificate of Correction effecting such corrections. Patentee respectfully solicits the granting of the requested Certificate of Correction.

The Commissioner is authorized to charge any deficiency of up to $300.00 or credit any excess in this fee to Deposit Account No. 04-0100.

Dated: February 15, 2007

Respectfully submitted,

By _____

Flynn Barrison
Registration No.: 53,970
DARBY & DARBY P.C.
P.O. Box 5257
New York, New York 10150-5257
(212) 527-7700
(212) 527-7701 (Fax)
Attorneys/Agents For Applicant

Issued Patent Proofing Form
Note: P = PTO Error A = Applicant Error

File#: 08223/000S102-US0

US Serial No.: **09/656,166** US Patent No.: **US 7,165,175 B1** Issue Dt.: **Jan. 16, 2007**

Title: **APPARATUS, SYSTEM AND METHOD FOR SELECTIVELY ENCRYPTING DIFFERENT PORTIONS OF DATA SENT OVER A NETWORK**

Sr. No.	P/A	Original		Issued Patent		Description of Error
		Page	Line	Column	Line	
1	P	Sheet 1 of 3 Information Disclosure Statement (IDS) Filed (07/29/2004)	Entry 21 (U.S. Patent Documents)	Page 2 Col. 1 (U.S. Patent Documents)	65	After "6,314,409" delete "B1" and insert - - B2 - -, therefor.
2	P	Sheet 2 of 3 Information Disclosure Statement (IDS) Filed (07/29/2004)	Entry 14 (U.S. Patent Documents)	Page 2 Col. 2 (U.S. Patent Documents)	3	After "6,409,080" delete "B1" and insert - - B2 - -, therefor.
3	P	Sheet 1 of 3 Information Disclosure Statement (IDS) Filed (07/29/2004)	Entry 26 (U.S. Patent Documents)	Page 2 Col. 2 (U.S. Patent Documents)	16	After "6,634,028" delete "B1" and insert - - B2 - -, therefor.
4	P	Sheet 2 of 3 Information Disclosure Statement (IDS) Filed (07/29/2004)	Entry 9 (U.S. Patent Documents)	Page 2 Col. 2 (U.S. Patent Documents)	20	After "6,654,423" delete "B1" and insert - - B2 - -, therefor.
5	P	Page 19 Specification (09/06/2000)	1	10	3	Delete "384," and insert - - 384; - -, therefor.
6	P	Page 20 Specification (09/06/2000)	19	10	61	After "another" delete ",".
7	A	Page 3 Claims (05/23/2006)	Claim 16 Line 1	12	13	In Claim 15, after "apparatus" delete "in" and insert - - is - -, therefor.
8	A	Page 13 Claims (05/23/2006)	Claim 78 Line 5	16	49	In Claim 74, delete "a" before "payload".
9	A	Page 16 Claims (05/23/2006)	Claim 97 Line 2	18	29	In Claim 92, before "examination" delete "an" and insert - - on - -, therefor.

PTO/SB/44 (04-05)
Approved for use through 04/30/2007. OMB 0651-0033
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.
(Also Form PTO-1050)

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO.	:	7,165,175
APPLICATION NO.	:	09/656,166
ISSUE DATE	:	January 16, 2007
INVENTOR(S)	:	Brad Kollmyer et al.

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

On the Original Issued Patent:

Page 2 Col. 1 (U.S. Patent Documents); Line 65; After "6,314,409" delete "B1" and insert - - B2 - -, therefor.

Page 2 Col. 2 (U.S. Patent Documents); Line 3; After "6,409,080" delete "B1" and insert - - B2 - -, therefor.

Page 2 Col. 2 (U.S. Patent Documents); Line 16; After "6,634,028" delete "B1" and insert - - B2 - -, therefor.

Page 2 Col. 2 (U.S. Patent Documents); Line 20; After "6,654,423" delete "B1" and insert - - B2 - -, therefor.

Column 10; Line 3; Delete "384," and insert - - 384; - -, therefor.

MAILING ADDRESS OF SENDER (Please do not use customer number below):
Flynn Barrison
DARBY & DARBY P.C.
P.O. Box 5257
New York, New York 10150-5257

Column 12; Line 13; In Claim 15, after "apparatus" delete "in" and insert - - is - -, therefor.

Column 16; line 49; In Claim 74, delete "a" before "payload".

Column 18; Line 29; In Claim 92, before "examination" delete "an" and insert - - on - -, therefor.

MAILING ADDRESS OF SENDER (Please do not use customer number below):
Flynn Barrison
DARBY & DARBY P.C.
P.O. Box 5257
New York, New York 10150-5257

U.S. PATENT DOCUMENTS

5,144,663 A 9/1992 Kudelski et al.
5,161,193 A * 11/1992 Lampson et al. 713/151
5,375,168 A 12/1994 Kudelski
5,420,866 A * 5/1995 Wasilewski 370/426
5,539,450 A 7/1996 Kudelski et al.
5,590,200 A 12/1996 Nachman et al.
5,592,212 A 1/1997 Handelman
5,621,799 A 4/1997 Katta et al.
5,640,456 A 6/1997 Adams, Jr. et al.
5,640,546 A 6/1997 Gopinath et al.
5,666,412 A 9/1997 Handelman et al.
5,678,002 A * 10/1997 Fawcett et al. 715/709
5,684,876 A 11/1997 Pinder et al.
5,758,257 A 5/1998 Herz et al.
5,774,527 A 6/1998 Handelman et al.
5,774,546 A 6/1998 Handelman et al.
5,796,836 A * 8/1998 Markham 380/28
5,799,089 A 8/1998 Kuhn et al.
5,805,705 A 9/1998 Gray et al.
5,878,134 A 3/1999 Handelman et al.
5,883,957 A 3/1999 Moline et al.
5,892,900 A 4/1999 Ginter et al.
5,910,987 A 6/1999 Ginter et al.
5,915,019 A 6/1999 Ginter et al.
5,917,912 A 6/1999 Ginter et al.
5,920,625 A 7/1999 Davies
5,920,861 A 7/1999 Hall et al.
5,922,208 A 7/1999 Demmers
5,923,666 A 7/1999 Gledhill et al.
5,933,498 A 8/1999 Schneck et al.
5,939,975 A 8/1999 Tsuria et al.
5,943,422 A 8/1999 Van Wie et al.
5,949,876 A 9/1999 Ginter et al.
5,982,891 A 11/1999 Ginter et al.
5,991,399 A * 11/1999 Graunke et al. 380/279
6,009,116 A 12/1999 Bednarek et al.
6,009,401 A 12/1999 Horstmann
6,009,525 A 12/1999 Horstmann
6,021,197 A 2/2000 von Willich et al.
6,035,037 A 3/2000 Chaney
6,038,433 A 3/2000 Vegt
6,044,468 A * 3/2000 Osmond 726/5
6,049,671 A 4/2000 Slivka et al.
6,055,503 A 4/2000 Horstmann
6,073,256 A 6/2000 Sesma
6,112,181 A 8/2000 Shear et al.
6,138,119 A 10/2000 Hall et al.
6,141,686 A * 10/2000 Jackowski et al. 709/224
6,154,840 A * 11/2000 Pebley et al. 713/160
6,157,721 A 12/2000 Shear et al.
6,178,242 B1 1/2001 Tsuria
6,185,683 B1 2/2001 Ginter et al.
6,189,097 B1 2/2001 Tycksen, Jr. et al
6,191,782 B1 2/2001 Mori et al.
6,226,794 B1 5/2001 Anderson, Jr. et al.
6,237,786 B1 5/2001 Ginter et al.
6,240,185 B1 5/2001 Van Wie et al.
6,247,950 B1 6/2001 Hallam et al.
6,253,193 B1 6/2001 Ginter et al.
6,256,668 B1 7/2001 Slivka et al.
6,272,636 B1 8/2001 Neville et al.
6,285,985 B1 9/2001 Horstmann
6,292,569 B1 9/2001 Shear et al.
6,298,441 B1 10/2001 Handelmann et al.
6,314,409 B1 11/2001 Schneck et al.
6,314,572 B1 11/2001 LaRocca et al.
6,334,213 B1 12/2001 Li
6,363,488 B1 3/2002 Ginter et al.
6,389,402 B1 5/2002 Ginter et al.
6,405,369 B1 6/2002 Tsuria
6,409,080 B1 6/2002 Kawagishi
6,409,089 B1 6/2002 Eskicioglu
6,424,717 B1 * 7/2002 Pinder et al. 380/239
6,427,140 B1 7/2002 Ginter et al.
6,449,367 B1 9/2002 Van Wie et al.
6,449,651 B1 * 9/2002 Dorfman et al. 709/229
6,449,719 B1 9/2002 Baker
6,459,427 B1 10/2002 Mao et al.
6,466,670 B1 10/2002 Tsuria et al.
6,505,299 B1 1/2003 Zeng et al.
6,587,561 B1 7/2003 Sered et al.
6,618,484 B1 9/2003 Van Wie et al.
6,629,243 B1 9/2003 Kleinman et al.
6,634,028 B1 10/2003 Handelmann
6,640,304 B1 10/2003 Ginter et al.
6,651,170 B1 11/2003 Rix
6,654,420 B1 11/2003 Snook
6,654,423 B1 11/2003 Jeong et al.
6,658,568 B1 12/2003 Ginter et al.
6,668,325 B1 12/2003 Collberg et al.
6,931,532 B1 * 8/2005 Davis et al. 713/167
2003/0007568 A1 1/2003 Hamery et al.

FOREIGN PATENT DOCUMENTS

EP 714204 B1 5/1996
WO WO-96/06504 A1 2/1996
WO WO-96/32702 A1 10/1996
WO WO-99/30499 A1 6/1999
WO WO-99/54453 A1 10/1999
WO WO-01/35571 A1 5/2001
WO WO-02/21761 A2 3/2002

OTHER PUBLICATIONS

Coverage and Generalization in an Artificial Immune System, Balthrop, et al., 2002.

Video Protection by Partial Content Corruption, C. Griwodz, Sep. 1998.

An Overview of Multimedia Content Protection in Consumer Electronics Devices, Eskicioglu et al.

Performance Study of a Selective Encryption Scheme for the Security of Networked, Real-Time Video, Spanos et al., 1995.

Goonatilake, Suran, ed. et al., Intelligent Systems for Finance and Business, 1995, chapters 2-10, pp. 31-173.

Irdeto Access and Optibase create Strategic Alliance—Dec. 14, 2000, http://www.irdetoaccess.com/press/0000041.htm.

System Security, Streaming Media, S. Blumenfeld, Oct. 2001. http://www.cs.unm.edu/~forest/projects.html, Doc. 2, 2003.

Partial Encryption for Image and Video Communication, H. Cheng, 1998.

A Review of Video Streaming Over the Internet, Hunter et al., Dec. 2, 2003.

Standards Track, Schulzrinne, et al., Apr. 1998, pp. 1-86.

http://www.optibase.com/html/news/December_14_2000.html, Dec. 14, 2004.

Omneon Video Networks Product Announcement, Broadband Streaming, pp. 1-4.

Yoshida, Kazuhiro. et al., "A Continuous-media Communication Method for Minimizing Playback Interruptions", IS&T/SPIE Conference on Visual Communications and Image Processing, Jan. 1999, San Jose, California, vol. 3653.

Communication pursuant to Article 96(2) EPC dated Jan. 26, 2006 (for EP Application No. 01968511.4).

PCT Notification of Transmittal Of The International Search Report; PCT/US 01/27518; Applicant: Widevine Technologies, Inc.; pp 1-7.

* cited by examiner

the firewall, proxy server or NAT that requires only the non-payload part to affect delivery to the user requesting the data stream.

A firewall, for example, does not recognize or try to block the encrypted data stream because the transport protocols do not define the appearance of the payload part, only the appearance of the non-payload part. The firewall looks at the non-payload part including but not limited to size, routing and header data. If the non-payload part data identify the data stream as a reply to a user request, then firewall **10** determines that the data stream is not malicious in origin and will not prevent it from going through. However, if the firewall is unable to parse the non-payload part or does not recognize the non-payload part than the data will be blocked from passing through.

In existing encryption solutions where the entire data portion of packets is encrypted, special modifications in each firewall, proxy server or NAT that the data stream might pass through are necessary. That is, the firewalls, proxy servers and NATs would have to be updated to identify the encrypted data. The present invention does not require modifications of the firewalls, proxy servers or NATs already deployed because it selectively encrypts the data packets leaving the portions important to firewalls, proxy servers and NATs unchanged such that the firewall, proxy server or NAT can pass the data stream to the intended target.

Some existing encryption solutions exist that encrypt only the media portion of a data stream by placing the encryption software on the streaming server as a plug-in to streaming server software, placing a heavy processing burden on the streaming server. This is in contrast to a benefit of the invention in that the invention can be used with a plurality of streaming servers without modification being required to the streaming servers and providing encryption without impacting the processing performance of the streaming servers.

Another feature of the invention is it provides a system that is independent in terms of the media format used. That is, the invention operates based on data protocol rather than file format. Multimedia streaming over networks is accomplished via several protocols. The invention recognizes the streaming protocol and acts on the data rather than requiring specific identification of the file format being transmitted. The invention is also independent in terms of the operating systems on the server machines since the invention requires no direct access to the server machines, the invention merely requires that the data streams from the streaming server pass through the EB.

The invention further provides a client system, also referred to as a decryption shim or simply a shim, which is a piece of transparent software that is downloaded to or pre-installed on the client machine (e.g. personal computer, network appliance or other network capable device) and used to decrypt incoming data streams from the EB on its way to the media player software. FIG. **3** is a flowchart of an exemplary decryption process of the decryption shim software performed at the client machine. The process comprises data streams as they are initiated **310**; determining whether the data is an encrypted stream **320**; ignoring the stream if it is not encrypted data **322**; determining if the encryption key is current **330**; negotiating a key with the encryption bridge/source if the key is not current **340**; parsing the data into payload and non-payload parts **350**; decrypting only the payload part **360**; passing the data to higher level operations (e.g. the media player) **370**; determining whether the data is the last part of a stream **380**; examining the operating environment for security **382**; determining if the client environment is compromised (hacked, etc.)**384**; shutting down the data stream if the client is compromised **385**; communicating with the encryption bridge/source **386**; resuming parsing data **388**; and terminating the stream if the data was the last part of the stream **390**.

Decryption is accomplished by adding a decryption shim **420** in a Layered Service Provider **410** in a Windows™ sockets network architecture as shown in FIG. **4** or a streams plug-in **510** in a streams based network architecture as shown in FIG. **5**. FIG. **4** is an exemplary diagram of a Windows™ sockets network architecture. In the Windows™ networking architecture, decryption shim **420** is the highest most Layered Service Provider (LSP) so that an additional LSP cannot merely spool decrypted data out into an insecure environment. This can be extrapolated to other sockets based networking protocols as well. FIG. **5** is an exemplary diagram of a streams based network architecture. The diagram represents placement of the invention's shim **520** within a streams based architecture **510** such as that employed by current incarnations of Mac OS™ and some versions of Unix.

When a user requests data that is encrypted by the EB of the invention, the transparent software is installed via an Active-X™ Control, a well documented means to deliver executable programs to a Windows™ computer. The installation of the decryption shim is transparent to the user and does not cause a reboot, restart of the user's browser or require user interaction. Some exceptions such as the Mac OS™ and Windows N™ or Windows 2000™ in secure environments or Linux or Unix based client machines because transparent installation requires administrative user privileges on the client machine and the ability of the client machine to receive programs via the Active-X™ mechanism.

After the last stream has finished, the decryption shim uninstalls as much of itself as possible, leaving only a small layer so that administrative user privileges are not required for future decryptions. The decryption shim is installed in volatile memory to reduce the changes of tampering by a third party.

After installation, the decryption shim decrypts only the data coming from the EB of the invention going to targeted players such as Windows Media™ Player, QuickTime™ Movie Player, Real Player™, etc. Decryption does not impact data targeted to other applications or media streams that are not encrypted by the EB of the invention.

The decryption shim runs on, for example, operating systems such as Windows 95™, Windows 98™, Windows ME™, Windows NT™, Windows 2000™ as well as Mac OS™ and numerous Linux and Unix distributions. Where Active-X™ based installation is possible, the installation of the decryption shim can be accomplished with most browsers such as Internet Explorer™ or Netscape™.

In sum, the EB of the invention drops in between the server and client and parses and encrypts a selected portion of the streamed data such as the media portion. As the stream is initiated, the decryption core is sent as part of the stream to the client side. The client can then decrypt the incoming data for the duration of the stream. If another stream is initiated, decryption occurs the same way. For each stream, the encryption keys can be set for the duration of the stream or changed during the stream duration to increase security.

As an example, a client may request privileges to get streaming data from a service provider's e-commerce system. The service provider's back-end (server infrastructure)

will authorize the streaming server to initiate a stream. That stream is initiated through the EB. Once initiated, the stream is parsed and selectively encrypted by the EB before being passed out over the network. Encryption keys are exchanged, for example, by the Diffie-Hellman mechanism that is known in the field. Unique features of the invention include the parsing and selective encryption of only the payload part of the data stream and the ability to plug-in other key exchange mechanisms and encryption algorithms should customer or security needs dictate.

It will be apparent to one of ordinary skill in the art that the embodiments as described above may be implemented in many different embodiments of software, firmware and hardware in the entities illustrated in the figures. The actual software code or specialized control hardware used to implement the present invention is not limiting of the present invention. Thus, the operation and behavior of the embodiments were described without specific reference to the specific software code or specialized hardware components, it being understood that a person of ordinary skill in the art would be able to design software and control hardware to implement the embodiments based on the description herein.

The invention claimed is:

1. An apparatus for selectively encrypting data for transmission over a network in packets between a server and a client, the apparatus comprising:

a parser configured to parse a payload portion of the data in a packet from a non-payload portion of the packet data;

an encrypter configured to determine if the payload portion of the packet data is to be encrypted by examining the payload portion of the packet data to recognize a predefined data type, and if it is to be encrypted, to encrypt the payload portion of the packet data; and

a data combiner configured to combine the encrypted payload portion of the packet data with the non-payload portion of the packet data, wherein the non-payload portion of the packet data includes more than routing information.

2. The apparatus of claim **1**, wherein the packet data includes streaming data.

3. The apparatus of claim **1**, wherein the non-payload portion of the packet data includes at least one of a header, control data and routing data.

4. The apparatus of claim **1**, further comprising a transmitter configured to send the combined payload and non-payload portions of the packet data over the network to the client

5. The apparatus of claim **1**, further comprising a receiver configured to receive the data from the server before the data is sent in the packet over the network to the client.

6. The apparatus of claim **1**, further comprising a device configured to establish a data stream between the server and the client

7. The apparatus of claim **1**, further comprising a key negotiator configured to negotiate an encryption key with the client.

8. The apparatus of claim **7**, wherein key negotiation and key exchange occur during transmission of a stream.

9. The apparatus of claim **8**, wherein the encrypter is transparent to the server.

10. The apparatus of claim **7**, wherein key negotiation can determine if the encryption key is current.

11. The apparatus of claim **1**, further comprising a decrypter configured to decrypt the encrypted payload portion of the packet data at the client.

12. The apparatus of claim **1**, wherein the parser is further configured to parse the packet data into different portions based on a media format.

13. The apparatus of claim **1**, wherein the encrypter is further configured to encrypt the payload portion of the packet data based on a media format.

14. The apparatus of claim **1**, wherein the apparatus is implemented utilizing an application that includes a pluggable core encoding an encryption algorithm for encrypting the payload portion of the packet data, wherein the pluggable core enables the encryption algorithm to be readily changed.

15. The apparatus of claim **1**, wherein the apparatus in implemented on an encryption bridge.

16. The apparatus of claim **1**, wherein the payload packet data includes multimedia data.

17. The apparatus of claim **1**, wherein the parser is further configured to parse the packet data into different portions based on a data protocol used to transmit a data stream of packets.

18. The apparatus of claim **1**, wherein the parser parses the packet data based on a data protocol.

19. A method for selectively encrypting data in a packet received from a data source, the data including payload and non-payload portions which differ from each other in at least one characteristic, the received data to be subsequently sent over a network to a client, the method comprising:

parsing the received packet data into portions including the payload and non-payload portions;

determining if the payload portion is to be encrypted based on a format of the payload portion of the packet data by examining the payload portion of the packet data to recognize a predefined data type, and if it is to be encrypted, encrypting the payload portion of the received packet data; and

sending the received packet data including the encrypted payload portion and the non-payload portion of the received packet data over the network to the client.

20. The metbod of claim **19**, wherein the data source is a server.

21. The method of claim **19**, further comprising determining whether a stream is established between a server and the client.

22. The method of claim **19**, further comprising negotiating an encryption key with the client.

23. The method of claim **22**, wherein the received packet data from the data source is streaming data sent during a streaming session and the negotiating of the encrypion key is carried out during the streaming session.

24. The method of claim **22**, wherein the received packet data from the data source is streaming data sent during a streaming session, the method further comprising examining the client during the streaming session and terminating the streaming session if the encryption key on the client is invalid.

25. The method of claim **22**, wherein the encryption key is negotiated with a decryption shim on the client.

26. The method of claim **19**, further comprising determining whether the received packet data is streaming data.

27. The method of claim **26**, further comprising parsing, encrypting and sending the packet data if the packet data is streaming data and sending the packet data if the packet data is not streaming data.

28. The method of claim **19**, further comprising determining whether a shim is present on the client.

58. An apparatus for selectively encrypting streaming data packets received from a streaming data source for transmission over a network to a client, the apparatus comprising:

a parser configured to parse a plurality of portions of the streaming data packets, wherein the plurality of portions include a payload portion and a non-payload portion in each of the streaming data packets;

an encrypter configured to encrypt at least the payload portion if it is determined, based on an examination of a format of the payload portion to recognize a predefined data type, payload portion is to be encrypted, but not encrypt at least one other data portion of the plurality of data portions; and

a data combiner configured to combine the encrypted payload portion with at least one unencrypted non-payload data portion.

59. The apparatus of claim 58, further comprising a negotiator, wherein the negotiator negotiates and exchanges a key with the client before the combined packet data is transmitted over the network to the client, the key enabling the client to decrypt the encrypted payload portion of the packet data for play on the client.

60. The apparatus of claim 59, wherein the streaming data is sent from the streaming data source during a streaming session.

61. The apparatus of claim 60, further configured to perform actions including examining the client during the streaming session and terminating the streaming session if the client has been compromised.

62. The apparatus of claim 58, wherein the at least one unencrypted data portion of the packet data includes at least one of a header, control data and routing data.

63. The apparatus of claim 58, wherein the streaming data source is at least one server.

64. An apparatus for selectively encrypting data received from a data source for transmission in packets over a network to a client, comprising:

a parser configured to parse at least two portions of the packet data, at least one of the two portions of the packet data including more than routing information for a packet;

an encrypter configured to determine if a payload portion of the packet data is to be encrypted based on an examination of the payload portion the packet data to recognize a predefined data type, and if it is to be encrypted, encrypting the payload portion of packet data not including the routing information for the packet; and

a data combiner configured to combine the parsed at least two portions of the packet data following encryption of the payload portion of data not including the routing information for the packet.

65. The apparatus of claim 64, wherein an unencrypted portion of the packet data includes at least one of a header and control data.

66. The apparatus of claim 65, wherein the parser parses the data into different portions based on a data protocol used to transmit the data.

67. The apparatus of claim 65, wherein the portion of the packet data to be encrypted includes media data encoded in a media format and wherein the encrypter encrypts the packet data to be encrypted based on the media format.

68. The apparatus of claim 67, wherein the apparatus is implemented utilizing an application that includes a pluggable core encoding an encryption algorithm for encrypting the packet data, the pluggable core being replaceable to enable the encryption algorithm to be readily changed.

69. The apparatus of claim 68, wherein the apparatus is implemented on an encryption bridge.

70. An apparatus for selectively encrypting data received from a data source during a downloading operation, the data being received from the data source for transmission in packets over a network to a client receiving the downloaded packetized data, comprising:

a parser configured to parse at least two portions of the data in a packet, wherein the packet data includes a payload portion and a non-payload portion;

an encrypter configured to determine if the payload portion of the packet data is to be encrypted based on a format of the payload portion of the packet data, wherein the format is determined based on an examination of the payload portion of the packet data to recognize a predefined data type, and if it is to be encrypted, encrypting the payload portion of the packet data; and

a data combiner configured to combine the encrypted payload portion of the packet data with an unencrypted portion of packet data for transmission over the network.

71. The apparatus as defined in claim 70, wherein the downloaded data is included in the encrypted payload portion of the packet data.

72. The apparatus of claim 71, wherein the unencrypted portion of packet data includes at least one of a header, control data and routing data.

73. The apparatus of claim 72, further comprising a key negotiator configured to perform actions including negotiating and exchanging a key with the client before the packet data is sent over the network to the client, the key enabling the client to decrypt the encrypted payload portion of data.

74. An apparatus for selectively encrypting data, received from a data source during a downloading operation and for selectively encrypting data received in packets from a data source during a streaming operation, the packet data being received from the data source for transmission over a network to a client receiving the downloaded or streaming data, comprising:

a means for parsing at least two portions of the data included in a packet, wherein the packet data comprises at least a payload portion and a non-payload portion;

a means for determining if the payload portion of the at least two portions of data is to be encrypted based on a format of the one portion of packet data that is determined by recognizing a predefined data type in the payload portion of the at least two portions, and if the payload portion of data is to be encrypted, employing a means for encrypting only the payload portion of the at least two portions of data; and

a means for combining the encrypted payload portion of the packet data with at least the unencrypted portion of the packet data for transmission over the network.

75. The apparatus of claim 74, wherein during the streaming operation, the streaming data is included in the packet data portion that is to be encrypted.

76. The apparatus as defined in claim 75, further comprising a key negotiating means configured to negotiate and exchange a key with the client before the streaming data is sent over the network to the client, the key enabling the client to decrypt the encrypted payload portion of the packet data for play on the client.

77. The apparatus of claim 74, further comprising a client examining means configured to examine the client during a streaming session and terminate the streaming session if the client has been compromised.

78. The apparatus of claim 77, wherein the packet data portion that is not encrypted includes at least one of a header, control data and routing data.

79. The apparatus of claim 74, wherein during a downloading operation, the downloaded data is included in the packet data portion that is to be encrypted.

80. The apparatus of claim 79, wherein the data portion that is not encrypted includes at least one of a header, control data and routing data.

81. A shim deployed on a client, the shim comprising:

a data receiver configured to receive partially encrypted packet data transmitted to the client, wherein another device parsed the packet data into a payload portion and a non-payload portion and determined the payload portion of the packet data to be encrypted based on a format of the payload portion of the packet data, wherein the format is determined by an examination of that payload portion of the packet data to recognize a predefined data type;

a parser configured to parse the partially encrypted packet data to select the payload portion of the packet data to be decrypted;

a decrypter configured to decrypt the payload portion of the packet data selected for decrypting by the parser; and

a data transmitter configured to send the decrypted packet data to a higher level operation resident on the client.

82. The shim of claim 81, wherein an encrypted portion of the transmitted packet data includes media data, the data transmitter being further configured to send the decrypted media data to a media player resident on the client.

83. The shim of claim 82, wherein the media data is streaming media transmitted to the client during a streaming session.

84. The shim of claim 83, wherein the unencrypted portion of the packet data includes at least one of a header, control data and routing data.

85. The shim of claim 83, further comprising an analyzer configured to analyze a behavior of the client to detect known media piracy techniques and to terminate the streaming session if a known media piracy technique is detected.

86. The shim of claim 83, further comprising an analyzer configured to analyze a behavior of the client to detect suspicious client behavior and to terminate the streaming session if specific behavior is detected.

87. The shim of claim 83, further comprising an analyzer configured to analyze a behavior of the client to detect known media piracy techniques and to terminate operation of at least the decrypter when a media piracy technique is detected.

88. The shim of claim 83, further comprising an analyzer configured to analyze a behavior of the client to detect suspicious client behavior and to terminate the operation of at least the decrypter if suspicious behavior is detected.

89. The shim of claim 83, further comprising a key negotiator configured to negotiate and exchange a key with the client before the packet data is sent over the network to the client, the key enabling the client to decrypt the encrypted portion of the packet data for play on the client.

90. The shim of claim 83, wherein the streaming data is sent to the client from an encryption source, the shim further including a key negotiator configured to negotiate and exchange a key with the encryption source, the key being used by the decrypter to decrypt the encrypted portion of the packet data.

91. The shim of claim 90 wherein the key negotiator is further configured to carry out the negotiating and exchanging of the key with the encryption source during the streaming session.

92. A method for providing data in packets over a network, comprising:

determining a plurality of portions of data in a packet that includes a payload portion and a non-payload portion;

determining if at least the payload portion of the plurality of portions of the packet data is to be encrypted based on examination of the payload portion, wherein the examination is to recognize a predefined data type and if the payload portion is to be encrypted, selectively encrypting the payload portion in the plurality of portions, wherein at least one other non-payload portion remains unencrypted;

authenticating a client to receive the packet that includes the selectively encrypted payload portion; and

transmitting the packet that includes the selectively encrypted payload portion to the authenticated client.

93. The method of claim 92, wherein authenticating the client further comprises the client accepting a shim transmitted from a server that is selectively encrypting the payload portion, and wherein the shim is configured to send back a confirmation.

94. The method of claim 92, wherein authenticating the client further comprises the client transmitting a self-generated certificate.

* * * * *